CLAIMS

What is claimed is:

1. An apparatus comprising:

a tamper resistant digital content recovery module to recover protected digital contents of various types in an obfuscated manner;

a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types, including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module;

one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules; and

a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules.

2. The apparatus of claim 1, wherein the tamper resistant module is equipped to verify to its satisfaction that the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having so verified to its satisfaction that the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised.

3. The apparatus of claim 2, wherein the tamper resistant module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy, responsive to a request from the plain text digital content rendering module occupying the root position of the hierarchy to recover a protected digital content.

4. The apparatus of claim 3, wherein the tamper resistant module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position.

5. The apparatus of claim 1, wherein each of at least a subset of the plain text digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream plain text digital content rendering module or modules, if any, have not been compromised.

6. The apparatus of claim 5, wherein each of the subset of the plain text digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream plain text digital content rendering module or modules have not been compromised, at least during initialization.

7. The apparatus of claim 6, wherein each of the subset of the plain text digital content rendering modules is equipped to further verify to its satisfaction that an immediate downstream plain text digital content rendering module or modules

remain un-compromised before each transfer of recovered digital content to the immediate downstream plain text digital content rendering module.

8. The apparatus of claim 5, wherein each of the subset of the plain text digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream plain text digital content rendering module or modules have not been compromised by verifying corresponding signature or signatures of the immediate downstream plain text digital content rendering module or modules.

9. The apparatus of claim 1, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

10. The apparatus of claim 1, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems.

11. The apparatus of claim 1, wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and a second subset of the plain text digital content rendering modules are member modules of a second application domain.

12. A processor implemented method, comprising:

a root one of a plurality of hierarchically organized plain text digital content rendering modules collectively equipped to render digital contents of a plurality of

types requesting a tamper resistant digital content recovery module to recover a first protected digital content of a first type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

the tamper resistant digital content recovery module recovering the first protected digital content in an obfuscated manner, and transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said first digital content, with each of said root and non-leaf ones, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

13. The method of claim 12, wherein the tamper resistant module verifies the root one of the plurality of hierarchically organized plain text digital content rendering modules by verifying its signature.

14. The method of claim 12, wherein each of said root and non-leaf ones, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules verifies an immediate downstream module is uncompromised by verifying the immediate downstream module's signature.

15. The method of claim 12, wherein the method further comprises each of said root and non-leaf ones, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules verifies its immediate downstream module or modules, if any, during initialization.

16. The method of claim 12, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

17. The method of claim 12, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of a second type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and non-leaf ones, if any, of said second at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

18. An apparatus comprising:

a plurality of digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of which to be selectively employed to protectively render digital contents of corresponding types, including one of said digital content rendering modules occupying a root position of the hierarchy to exclusively receive the digital

contents to be rendered, of all types, from at least a separate recovery module responsible for recovering the digital contents from their ciphered states, and each of the non-leaf ones of the digital content rendering modules being responsible for verifying to its own satisfaction that its immediate downstream module or modules, if any, have not been compromised;

one or more storage units to store said plurality of digital content rendering modules; and

a processor coupled with the one or more storage units to execute the digital content rendering modules.

19. The apparatus of claim 18, wherein each of the non-leaf ones of the digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream module or modules, if any, have not been compromised, at least during initialization.

20. The apparatus of claim 18, wherein each of the non-leaf ones of the digital content rendering modules is equipped to further verify to its satisfaction that an immediate downstream digital content rendering module remains uncompromised before each transfer of digital contents to the immediate downstream digital content rendering module.

21. The apparatus of claim 20, wherein each of the non-leaf ones of the digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream digital content rendering module or modules, if any, have not been compromised, by verifying corresponding signature or signatures of the immediate downstream digital content rendering module or modules.

22. The apparatus of claim 18, wherein the digital content of various types comprises streaming media contents of a plurality of media types, and of a plurality of format types.

23. The apparatus of claim 18, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems.

24. The apparatus of claim 18, wherein a first subset of the non-leaf modules are member modules of a first application domain, and a second subset of the non-leaf modules modules are member modules of a second application domain.

25. A processor implemented method comprising

each of a plurality of hierarchically organized digital content rendering modules verifying to its satisfaction that each of its immediate downstream module, if any, is uncompromized, during an initialization period;

a root one of the plurality of hierarchically organized digital content rendering modules exclusively receiving a first digital content of a first type; and

said root one in conjunction with first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said first digital content, with each of said root and non-leaf ones, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules further verifying an immediate downstream module is uncompromised before transferring

the first digital content to the immediate downstream module to further the rendering of the first digital content.

26. The method of claim 25, wherein each of said root and non-leaf ones, if any, of said first other ones of said plurality of hierarchically organized digital content rendering modules verifies an immediate downstream module is uncompromised by verifying the immediate downstream module's signature.

27. The method of claim 25, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of the same first type; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of the first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

28. The method of claim 25, wherein the method further comprises

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of a second type; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said

second digital content, with each of said root and non-leaf ones, if any, of the second at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

29. An article of manufacture comprising:

a recordable medium;

a first plurality of programming instructions recorded on said recordable medium, with said first programming instructions designed to program a computing device, to implement on the computing device, a tamper resistant digital content recovery module to recover protected digital contents of various types in an obfuscated manner; and

a second plurality of programming instructions recorded on said recordable medium, with said second programming instructions designed to program a computing device, to implement on the computing device, a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types, including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from a tamper resistant digital content recovery module.

30. The article of claim 29, wherein the tamper resistant module is equipped to verify to its satisfaction that the plain text digital content rendering module occupying

the root position of the hierarchy has not been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having so verified to its satisfaction that the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised.

31. The article of claim 29, wherein each of at least a subset of the plain text digital content rendering modules is equipped to verify to its satisfaction that the immediate downstream plain text digital content rendering module or modules, if any, have not been compromised.

32. The article of claim 29, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

33. The article of claim 29, wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium.